There may well be other legislative solutions that could be used against fraud, and MCI looks forward to the opportunity to address them in the future.

X. CONCLUSION

Toll fraud is a significant industry problem that requires the attention and resources of telecommunication service providers, consumers and government. To those ends, MCI urges the Commission to adopt policy, programs and rules, if necessary, in accordance with these Comments.

Respectfully submitted,

MCI TELECOMMUNICATIONS CORPORATION

By: Mary J. Sisak

Mary J. Sisak
Donald J. Elardo
1801 Pennsylvania Avenue, N.W.
Washington, D.C. 20006
(202) 887-2605

Dated: January 14, 1994

ATTACHMENT A

MCI Helps Your Put The Finger On Fraud

MCI DETECT

Telecommunications Fraud Protection

YOUR PARTNER IN TELECOMMUNICATIONS FRAUD PREVENTION

CPE-RELATED FRAUD...A COSTLY, GROWING PROBLEM

CPE-related fraud, the illegal use of private telecommunications systems, can be a serious problem for owners of Customer Premises Equipment (CPE) such as PBX and voice mail systems. Surreptitiously tapping into systems through electronic "hacking" or by stealing access codes, these thieves are able to use someone else's phone lines to place costly international calls.

Many of them sell overseas calls at bargain rates to street customers...others use the access for their own purposes, such as making non-traceable calls to drug dealers in foreign countries. It's not until weeks later, when unauthorized long-distance calls show up on phone bills, that unsuspecting companies find out that they've been victimized.

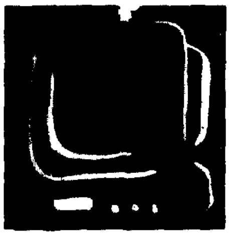
MCI DETECT: A MULTI-DISCIPLINARY APPROACH

MCI has developed MCI Detect,℠ a multi-disciplinary attack on the problem of fraud. This value-added approach for our customers is provided at no additional cost. It includes:

- Customer Awareness and Education
- CPE Fraud Detection Equipment
- Analysis of Customer Traffic
- Third Party Insurance

These elements are now being implemented and shared with our customers. Working with you as part of your fraud control team, MCI will do as much as we can to help you limit your exposure and financial loss. To find out what you can do to control fraud, take advantage of the MCI Detect program now.

CUSTOMER AWARENESS AND EDUCATION



Exclusive fraud awareness video for MCI customers.

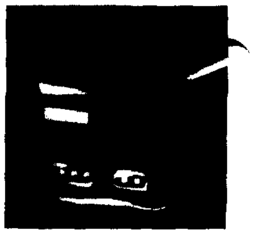
- Exclusive fraud awareness video for MCI customers
- Manual on easily compromised CPE features
- Newsletter on latest fraud control techniques

Securing Your CPE...the First Line of Defense

Awareness of fraud potential is critical to its detection. A new fraud awareness video presentation, "Invisible Criminals," is available to all MCI customers. MCI has played a leading role in educating customers to fraud potential and in ways to identify and control it. Over the past three years, fraud workshops have been held for more than 2,000 participants.

The first and most important barrier to telephone fraud is to secure your CPE. The <u>MCI Detect</u> newsletter will keep you updated on the latest techniques, technology and ideas. A manual for MCI customers explaining the features of CPE which are vulnerable to attack will be available mid 1993. MCI can also provide security consulting assistance on a special case basis for customers who have more complex systems.

CPE FRAUD DETECTION EQUIPMENT THROUGH AFFILIATES PROGRAM



20% discount on recommended CPE-attached hardware.

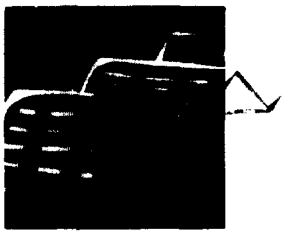
- 20% discount on recommended CPE-attached hardware
- Monitoring of PBX traffic on a real time basis

The First Signs of Fraud Can Be Costly

Usually, the first signs of fraud are unexpected spikes in telephone usage along with a sudden rise in calls to certain areas. But these indicators often become apparent weeks after the fact, when much of the damage has already been done. A more timely, continuous analysis of traffic can be accomplished with PBX add-on equipment.

State-of-the-art access control and outbound traffic monitoring are available through equipment manufactured by MicroFrame and Xiox. These units monitor PBX traffic on a real-time basis. When thresholds are triggered, the equipment sends alarms and can even take the ultimate measure of shutting down the abused facility without human intervention. MCI currently uses both MicroFrame and Xiox equipment on its own office PBXs, and has arranged a 20% discount on CPE-attached hardware units for MCI customers.

ANALYSIS OF CUSTOMER TRAFFIC



MCI monitoring program helps spot possible fraud.

- Analysis of outbound international and inbound 800 traffic to determine fraudulent usage patterns
- Customer notification of suspected fraud
- Assistance with identifying how CPE was compromised

MCI Program Helps Spot Possible Fraud

Fraud can still occur, no matter how carefully access to long distance lines is controlled. A hacker can get lucky, new technology may be able to subvert yours, disgruntled employees may sell codes...the possibilities are endless.

A program of recording and analyzing customers' usage in an effort to detect traffic with high-fraud-potential allows MCI to spot suspicious calling patterns and advise customers before the charges appear on their bills. There is no charge to the customer for this service and gradual extension is planned as technology permits. It's another part of MCI's commitment to our customers.

THIRD-PARTY INSURANCE

MCI works or non-restrictive raud insurance.

- True insurance that transfers risk
- Coverage of <u>any</u> long distance carriers' traffic

Industry efforts have been made to limit fraud loss through service guarantees that function similarly to insurance coverage. However, these plans are limited to specific carriers and require specific volume traffic commitments.

MCI has a working relationship with an insurance broker, Henry Ward Johnson & Company, Inc.; and a major insurance company for the introduction of an insurance policy which transfers fraud risk without these shortcomings. MCI does not view insurance as a sales tool. We want all our customers, no matter how many carriers they may be using, to have maximum protection and minimum loss.

FOR MORE INFORMATION, TALK TO YOUR MCI REPRESENTATIVE.

We'll work with you in every way possible to reduce the risk of CPE-related fraud loss. Through MCI Detect, MCI makes its expertise on CPE-related fraud available to its customers at no additional charge.

As an MCI customer, MCI Detect will help you plan and implement a fraud prevention program tailored expressly to your needs. We will keep you abreast of new developments, emerging technologies, fresh ideas and effective solutions. We'll do everything we can to help you make your own program effective and cost efficient.

MCI DETECT

Telecommunications Fraud Protection

ATTACHMENT A

MCI

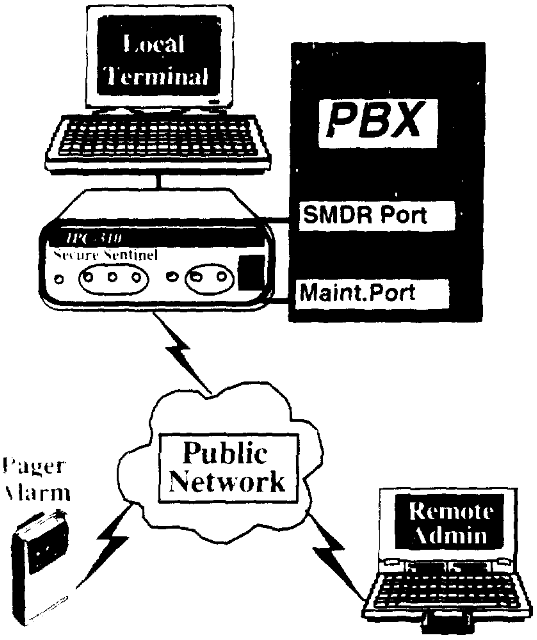
In Affiliation With

MicroFrame

No Additional Lines, Easy Installation and Initialization

Both the remote access maintenance port and SMDR port connect to the IPC-310 eliminating the cost of extra support lines and modems. Initialization is easily accomplished through a series of menu-driven prompts.

Any combination of available authentication technologies may be selected for maintenance port access. Up to 20 user-defined CDR control parameters are available for setting alarm criteria, including both percent deviation from normal profiles and number-of-events limitations in each parameter.



Technical Specifications

Basic Secure Sentinel© IPC-310 Platform

Authentication Models	**Type**
Callback:	Fixed/Variable Callback, Password Only
Direct Dial Token:	In-Line: TeleKEY MagnaKEY SofKEY Off-Line: PassKEY and Other Popular Tokens
Operating Characteristics	
Internal Modem:	2400 bps with MNP level 5 Error Correction ANI Compatible
Maximum Link Speed:	19.2 Kbps. Speed Matching between Ports
Data Connections:	Host 1-RS-232/DB25S, Host 2-RS232/DB9S Aux Port-RS-232/DB25S
Analog Connections:	RJ11
Standard Display:	Red, Green, Yellow LED Indicators
Standard Power:	110/220/240 VAC. 50/60 Hz
Optional Power:	48V to 52V DC
Back-up Power:	Holdover Battery included
Standard Memory:	1MB Battery Supported Static RAM
Buffer memory:	Programmable
Temperature Range:	0-40 degrees Centigrade
Relative Humidity:	To 95%, non-condensing
Dimensions	5.75"x9.50"x2.75"

FOR INFORMATION

CALL 1(800)395-7450

MicroFrame, Inc.
21 Meridian Road
Edison, NJ 08820

MCI®

MCI

Telecommunications Fraud Protection

MCI Helps You Put the Finger on Fraud

Customer Awareness and Education

- Exclusive fraud awareness video for MCI customers
- Manual on easily-compromised CPE features
- Newsletter on latest fraud control techniques

CPE Fraud Detection Equipment Through Affiliates Program

- 20% discount on recommended hacker prevention hardware
- Monitoring of PBX traffic on a real-time basis

Analysis of Customer Traffic

- Analysis of outbound international and inbound 800 traffic to detect fraudulent usage patterns
- Customer notification of suspected fraud
- Assistance with identifying how CPE was compromised

Third-Party Insurance

- True insurance that transfers risk
- Coverage of any long distance carriers' traffic

MCI offers its MCI Detect in an effort to help its customers to help fight against fraud, but it does not undertake itself to guarantee to customers that this program will successfully prevent fraud.

MCI®

© MCI Telecommunications Corporation [illegible]

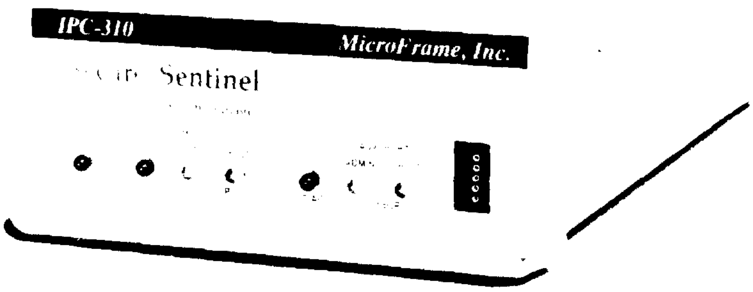
MCI

In Affiliation With

MicroFrame

IPC-310 SECURE SENTINEL

Dual-port controller with internal modem provides continuous toll fraud loss control through real-time call-detail monitoring, maintenance port security, and alarm management.



The MicroFrame Secure Sentinel integrates the essential elements of a sound telephone fraud loss-prevention program into a single solution. The Secure Sentinel connects to both the SMDR and the maintenance port of the PBX, securing the maintenance port against unauthorized access and detecting fraudulent activity by continuously monitoring call detail records. It provides prompt control action through alarms to PCs, pagers or FAX machines. If there is no response to the initial alarm within a pre-selected time, Secure Sentinel escalates alarms to higher authority and/or can automatically disable the abused facility.

MicroFrame has been a leader in programmable computer and data network security systems since 1982. Companies of all sizes rely on the Secure Sentinel as a key element in their fraud loss-control program.

Installation and initialization is quick and easy. For more information, contact MicroFrame, Inc. at 1-800-395-7450.

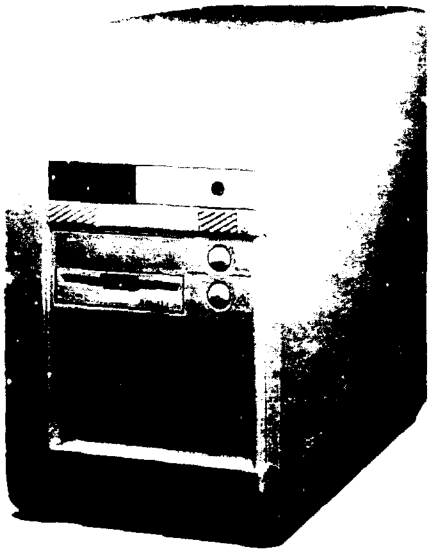
Realize the Following Benefits

- ous monitoring and analysis of call-ecords to determine if activity exceeds ned threshold levels
- l access to PBX maintenance ports dvanced caller authentication dogies
- t activity captured and logged
- ent "auto-learn" mode to establish rofiles
- atic alarm notification to PC, pager X
- tion of alarms to higher level if no e within selected time frame
- atic shut-down capability if no e to alarms
- l 20% discount on entire line of Frame products for all MCI customers

MCI

In Affiliation With

Xiox



THE HACKER PREVENTER

Advanced artificial intelligence provides continuous, high level security against fraudulent access to PBX.

The Xiox Hacker Preventer provides a unique, proactive approach to telecommunications fraud control. Using three lines of defense, it guards inbound access to PBX systems, blocking the efforts of even highly sophisticated hackers. This is achieved through a combination of user ID, password, and verbal authorization, making the probability of guessing a valid code one in a billion. Repeated access attempts and unusual call patterns are recognized and access is denied.

Drawing upon experience and expertise gained over more than a decade of providing PC-based call accounting and telecommunications security, Xiox offers a complete family of hardware and software for successfully blocking, tracking and trapping hackers and system abusers. In addition to the Hacker Preventer, the Fort Knox family includes the Hacker Deadbolt and the Hacker Tracker.

Realize The Following Benefits

- Three levels of inbound protection from telephone hackers
- Secure, monitored use of DISA-type features for traveling employees and telecommuters
- Automatic recognition of user-profile deviations and termination of fraudulent use
- On-demand printed reports for assistance with fraud analysis and usage research
- Secure access to remote maintenance ports, voice mail systems and modem pools
- Full realization of cost savings inherent to remote access systems
- Special 20% discount on entire family of XIOX products to all MCI customers

Easy Installation and Custom Configuration

Within hours, the Xiox Hacker Preventer can be installed and configured to meet the precise security needs of your organization. The unit connects between one and sixteen extensions to your PBX and requires no special trunking or custom facilities. It can accommodate over 2,000 busy hour calls (depending on model) with the DIT feature. Configuration and maintenance can be accomplished either by standard telephone or by using the DOS-based configuration utility provided with the Hacker Preventer.

MCI

In Affiliation With

Xiox

- Stop inbound hackers...three levels of access protection include user ID and password, verbal password, and alarms.
- Stop outbound hackers...user IDs can be assigned to predefined classes of service for specific destinations such as interoffice or certain area codes, or restricted from access certain destinations such as international or any long distance calls.
- Stop hackers who don't trip alarms when leaving system proprietary user profiling, automated accumulation of profiles, and artificial intelligence comparisons to profile separate hackers from users.
- Stop hackers who try to reconfigure the user system. the remote maintenance port is protected by an array of password alternatives: a dial back modem capability and passwords in effect for limited periods such as one-time or 24-hour use
- Track hackers...robust reporting capabilities include Authorized User, Call Detail, Active User IDs, and Daily Activity by User ID.

Blocking...	The XIOX system that will... Track	Stop
Hackers who trip alarms accessing the system	XHP	XHP
Hackers who trip alarms leaving the system	XHP/ XHT	XHP
Hackers who don't trip alarms	XHP	XHP
Hackers who try to reconfigure the user's system	XHP/ XHDB	XHP/ XHDB

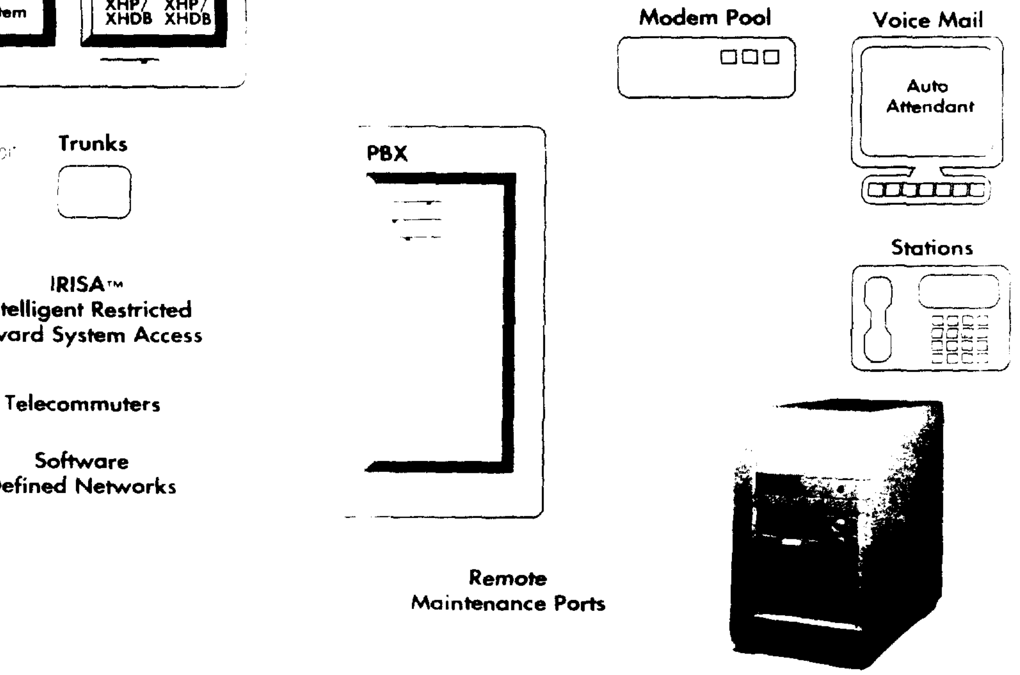
MATRIX KEY:

XHT= Xiox Hacker Tracker XHDB= Xiox Hacker Deadbolt

Technical Specifications

The Hacker Preventer™

Physical	Housing: Shelf or desk mounted enclosure
	H 13.5 in W 7.5 in D 16 in
	Weight exclusive of packing materials 28 pounds
Electrical	Mains power 115/230 Vac 50-60 Hz 50 VA max
	25 VA typical
Environment	Operating temperature 10-50 deg C
	Relative Humidity 10-95%
Telephone	RJ11 analog FCC registration EMC54S-15118-MD-E
	Recv 0.8B ULE10 1818
Functional	User ID code length: 8 digits maximum 1 digit minimum
	Dialed number length 28 digits maximum
	Global Service Classes 0 restricted 1&2 unrestricted
	User Service Classes 0 restricted, 1-9 unrestricted
Reports	Authorized User ID list, selectable by range of user code
	Call detail report, last in-first out 5000 call sliding window
	Active User Report, selectable by range of user code
	Daily Active User Report



FOR INFORMATION

CALL 1(800)685-8188

XIOX Corporation
577 Airport Blvd., Suite 700
Burlingame, CA 94010

MCI DETECTOR

[illegible]

A publi[illegible]
on the [illegible]
Te[illegible]commun[illegible]
[illegible]

Welcome to the New *MCI* *Detector*

This is the first editi[illegible] MCI Detect newsletter, DETE[illegible]TOR. We have designed this publication to provide you with an o[illegible]erview of MCI's fraud prevent[illegible] fea-tures, information on the latest fr[illegible]dulent tech-niques, helpful hints on how [illegible] fraud and feature stories on [illegible] helped customers.

A *growing number of compan[illegible]* [illegible] confronted with the toll fraud pr[illegible]blem. Wh[illegible] estimates vary, it is generally ackn[illegible] that CPE-related fraud accounts for [illegible] billion each year in losses. The [illegible] being hacked is very real.

MCI has a long history of helpin[illegible] deal with fraud problems includ[illegible] fraud prevention seminars, pro[illegible] consulting and supplying educati[illegible]al[illegible].

Now a new generation of anti fr[illegible] have been developed to combat [illegible]. MCI Detect is a value-added ser[illegible] to "HELP YOU PUT THE FIN[illegible] FRAUD." It is a multi-faceted app[illegible] sisting of 4 key elements:

1. Customer Aw[illegible] & Education — Free to MCI Cus[illegible]

- Exclusive, award winning, fraud [illegible] video, "Invisible Criminals
- MCI DETECTOR, quarterl[illegible] newsletter
- Manual on easily compromised CPE [illegible] and functions (available [illegible])
- "Hands on" consulting

2. Analysis of Custo[illegible] Traffic — Free to MC[illegible] Customers!

- Analysis of customer's MCI [illegible] originated 800 traffic and outb[illegible] national to select high-fraud [illegible]
- Customer notification of potentially fraud-ulent usage
- *Assistance in resolving fraudulent situations*

3 CPE Add-on Equip[illegible] through Affiliates Program

- *20% discount on MicroFrame and Niox* equipment for MCI customers
- Monitors any traffic routed through it; is not exclusive to the traffic of MCI or any other carrier
- Can be set to take corrective action without human intervention
- Has thresholds that can be tailored to indi-vidual business traffic patterns
- Monitors traffic on real time basis

4 Third-Party Insurance

- Coverage of all of customer's long distance traffic
- No MCI requirement for traffic volume commitment
- *True insurance, not a service guarantee*

For more information on how MCI Detect can help you put the finger on fraud speak with your MCI representative.

MCI intercepts fraudulent activity on *Times Record* in Maine 1-800 service and prevents thousands of dollars in losses.

hints

MCI has a long history of helping our customers with fraud problems.

DISA

Fraud Method(s) — DISA is designed to allow remote access to a PBX and then originate an outbound call. As a result of this design, many PBX owners use DISA in lieu of Calling Cards; however, it is also used by call sell operators in placing fraudulent calls.

The hackers are able to locate the DISA feature with the use of a "war dialer." The war dialer" dials telephone numbers randomly, generally 800 numbers, until a carrier or dial tone is obtained. After a number is found, hacking software is then used to search for valid authorization codes (auth codes). These codes are "frequently" but not always distributed to pirated voice mail systems and computer bulletin boards. The codes are rapidly distributed to a network of call sell operators and may also be posted on bulletin boards and voice mail systems

Fraud Solution(s) — There are many steps a PBX owner can take to prevent hackers from obtaining and fraudulently using the DISA feature. To begin with auth codes should be made as long as possible. At the very least a factor of 10,000 should exist between active codes. For example, if there are 10 users the code should be at least 7 digits (10 x 10,000 + 100.00 or 5 digits). Auth codes should be randomly scattered throughout the possible range but not easily defined (e.g. 1234 or 1111). Class of service restrictions should be applied to the auth codes. Only those with a truly legitimate need should be allowed International dialing through the DISA. A monitoring system should be set up to record DISA usage. Monitoring reports should show the number of times and duration each auth code is used in a day. If possible, the dollar value of those calls should also be noted in the reports.

Voice Mail Boxes (VMB) As Bulletin Board

Fraud Method(s) — There are two types of VMB Systems fraud. The first type occurs when a hacker takes over a box and uses it to communicate with other hackers. This can be expensive if access is gained to the VMB system via an 800 number. In this situation, a hacker typically hacks out the box password and changes it along with the greeting.

Fraud Solution(s) — To protect against a VMB being pirated the following steps should be taken:

- Do not allow administrative access via the phone. If telecom person can add, delete and change boxes via the phone, so can a hacker.
- Do not have active mail boxes that do not have an owner.
- Passwords should be at least 6 digits long.
- If possible, passwords should expire every 30-90 days.

Voice Mail Boxes (VMB) Garnering Dial Tone

Fraud Method(s) — The second type of abuse involves garnering a PBX dial tone via the VMB. This is accomplished in two ways. Both methods can transfer out of the VMB to a phone on the system. If the PBX is not set up properly the transfer can be made directly to dial tone. In other instances the caller transfers to an extension. In some cases the extension may be on another PBX and require transmission over a tie line. If the tie line is not properly secured, dial tone can be retrieved and fraudulent calls placed. Finally, all PBXs have Trunk Access Codes (TACs) or Facility Access Codes (FACs). Technicians use these codes to make test calls. If allowed, a hacker can transfer out of the VMB to the TACs or FACs.

Fraud Solution(s) — Steps to Prevent PBX Fraud:

- Disabling the transferring out feature. This would restrict use to only receiving and retrieving messages.
- Limiting access to only 4-digit extensions if transferring is allowed.
- Blocking 8 & 9 access (8 & 9 generally being draw dial tone numbers).
- Prohibiting trunk-to-trunk access to tie lines.
- Disallowing TAC and FAC access from the VMB.

ATTACHMENT A

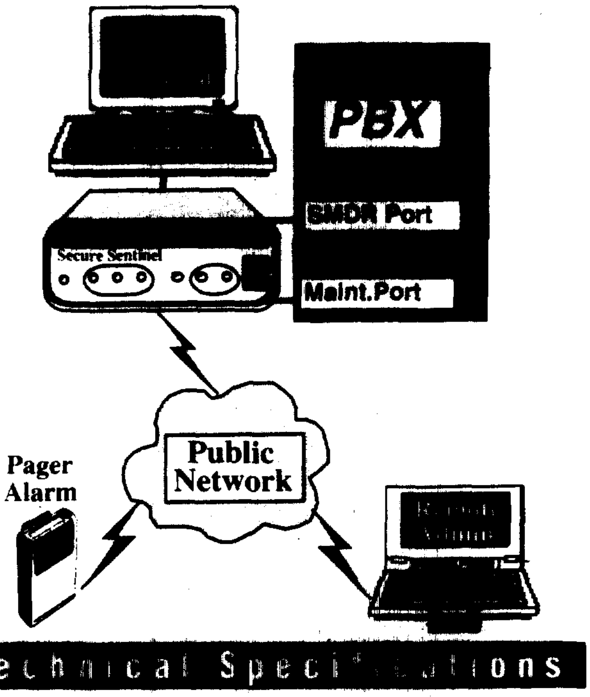
MCI

MicroFrame

No Additional Lines, Easy Installation and Initialization

Both the remote access maintenance port and SMDR port connect to the IPC-310, eliminating the cost of extra support lines and modems. Initialization is easily accomplished through a series of menu-driven prompts.

Any combination of available authentication technologies may be selected for maintenance port access. Up to 20 user-defined CDR control parameters are available for setting alarm criteria, including both percent deviation from normal profiles and number-of-events limitations in each parameter.



Technical Specifications

Basic Secure Sentinel© IPC-310 Platform

Authentication Models	**Type**
Callback:	Fixed/Variable Callback, Password Only
Direct Dial Token:	In-Line: TeleKEY, MagnaKEY, SofKEY Off-Line: PassKEY and Other Popular Tokens
Operating Characteristics	
Internal Modem:	2400 bps with MNP level 5 Error Correction ANI Compatible
Maximum Link Speed:	19,2 Kbps, Speed Matching between Ports
Digital Connections:	Host 1-RS-232/DB25S, Host 2-RS232/DB9S Aux Port-RS-232/DB25S
Analog Connections:	RJ11
Standard Display:	Red, Green, Yellow LED Indicators
Standard Power:	110/220/240 VAC, 50/60 Hz
Optional Power:	48V to 52V DC
Back-up Power:	Holdover Battery included
Standard Memory:	1MB Battery Supported Static RAM
Buffer memory:	Programmable
Temperature Range:	0-40 degrees Centigrade
Relative Humidity:	To 95%, non-condensing
Dimensions	5.75"x9.50"x2.75"

FOR INFORMATION
CALL 1(800)395-7450
MicroFrame, Inc.
21 Meridian Road
Edison, NJ 08820

MCI®

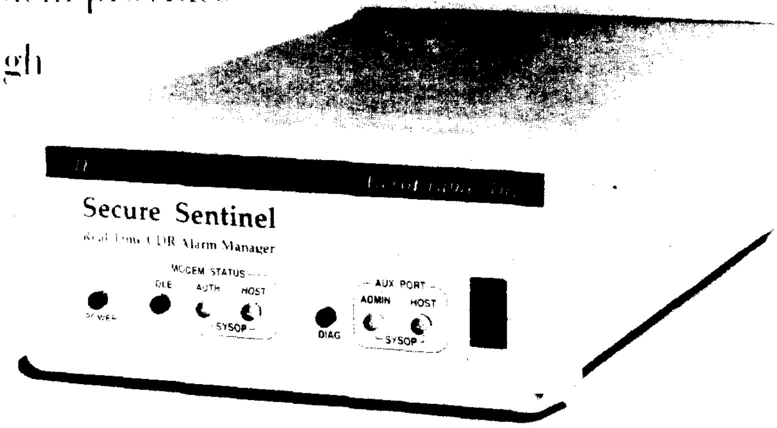
Control No. 20017 5/93

MCI

MicroFrame

IPC-310 SECURE SENTINEL

Dual-port controller with internal modem provides continuous toll fraud loss control through real-time call-detail monitoring. maintenance port security. and alarm management.



The MicroFrame Secure Sentinel integrates the essential elements of a sound telephone fraud loss prevention program into a single solution. The Secure Sentinel connects to both the SMDR and the maintenance port of the PBX. securing the maintenance port against unauthorized access and detecting fraudulent activity by continuously monitoring call detail records. It provides prompt control action through alarms to PCs. pagers or FAX machines. If there is no response to the initial alarm within a pre-selected time. Secure Sentinel escalates alarms to higher authority and/or can automatically disable the abused facility.

MicroFrame has been a leader in programmable computer and data network security systems since 1982. Companies of all sizes rely on the Secure Sentinel as a key element in their fraud loss control program.

Installation and initialization is quick and easy. For more information. contact MicroFrame, Inc.. at 1(800)395-7450.

Realize the Following Benefits

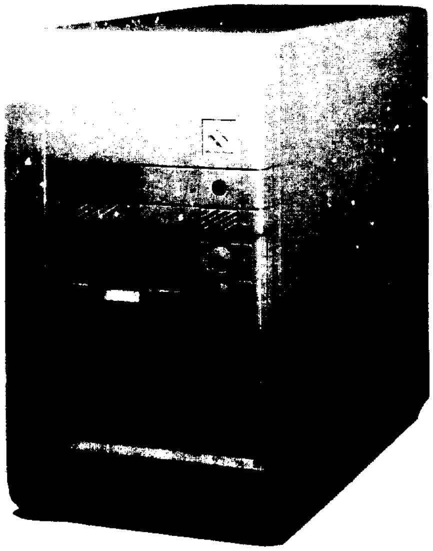
- Continuous monitoring and analysis of call-detail trends to determine if activity exceeds predefined threshold levels
- Secured access to PBX maintenance ports using advanced caller authentication technologies
- All port activity captured and logged
- Intelligent "auto-learn" mode to establish CDR profiles
- Automatic alarm notification to PC, pager or FAX
- Escalation of alarms to higher level if no response within selected time frame
- Automatic shut-down capability if no response to alarms
- Special 20% discount on entire line of MicroFrame products for all MCI customers

MCI

Xiox

THE HACKER PREVENTER™

Advanced artificial intelligence provides continuous, high level security against fraudulent access to PBX.



The Xiox Hacker Preventer provides a unique, proactive approach to telecommunications fraud control. Using three lines of defense, it guards inbound access to PBX systems, blocking the efforts of even highly sophisticated hackers. This is achieved through a combination of user ID, password, and verbal authorization, making the probability of guessing a valid code one in a billion. Repeated access attempts and unusual call patterns are recognized and access is denied.

Drawing upon experience and expertise gained over more than a decade of providing PC-based call accounting and telecommunications security, Xiox offers a complete family of hardware and software for successfully blocking, tracking and trapping hackers and system abusers. In addition to the Hacker Preventer, the Fort Knox family includes the Hacker Deadbolt and the Hacker Tracker.

Realize The Following Benefits

- Three levels of inbound protection from telephone hackers
- Secure, monitored use of DISA-type features for traveling employees and telecommuters
- Automatic recognition of user-profile deviations and termination of fraudulent use
- On-demand printed reports for assistance with fraud analysis and usage research
- Secure access to remote maintenance ports, voice-mail systems and modem pools
- Full realization of cost savings inherent to remote access systems
- Special 20% discount on entire family of XIOX products to all MCI customers

Easy Installation and Custom Configuration

Within hours, the Xiox Hacker Preventer can be installed and configured to meet the precise security needs of your organization. The unit connects between one and sixteen extensions to your PBX and requires no special trunking or telecomm facilities. It can accommodate over 2,000 busy hour calls (depending on model) through the DIT feature. Configuration and maintenance can be accomplished either by secure telephone or by using the DOS-based configuration utility provided with the Hacker Preventer.

MCI

Xiox

- Stop inbound hackers...three levels of access protection include user ID and password. verbal password. and alarming.
- Stop outbound hackers...user IDs can be assigned to nine defined classes of service for specific destinations such as interoffice or certain area codes. or restricted from access to certain destinations such as international or any long distance calls.
- Stop hackers who don't trip alarms when leaving system... proprietary user profiling. automated accumulation of profiles. and artificial intelligence comparisons to profiles separate hackers from users.
- Stop hackers who try to reconfigure the user system... the remote maintenance port is protected by an array of password alternatives: a dial back modem capability and passwords in effect for limited periods such as one-time or 24-hour use.
- Track hackers...robust reporting capabilities include Authorized User. Call Detail. Active User IDs. and Daily Activity by User ID.

The XIOX system that will...

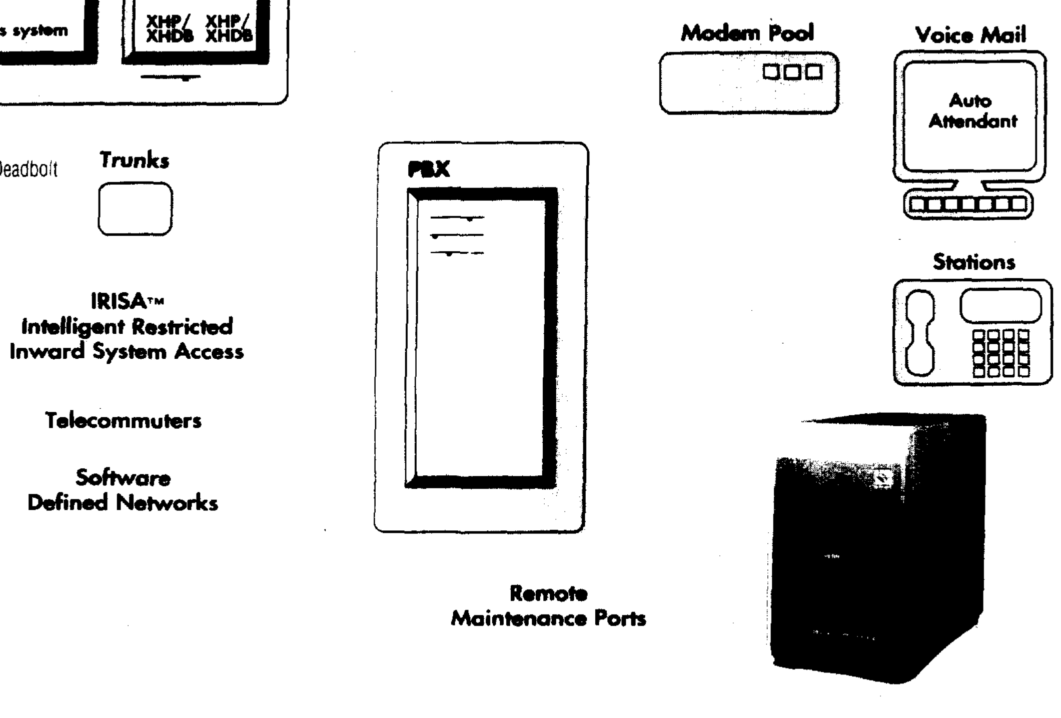
Blocking...	Track	Stop
Hackers who trip alarms accessing the system	XHP	XHP
Hackers who trip alarms leaving the system	XHP/ XHT	XHP
Hackers who don't trip alarms	XHP	XHP
Hackers who try to reconfigure the user's system	XHP/ XHDB	XHP/ XHDB

MATRIX KEY:
XHT= Xiox Hacker Tracker XHDB= Xiox Hacker Deadbolt

Technical Specifications

The Hacker Preventer™

Physical	Housing: Shelf or desk mounted enclosure H 13.5 in. W 7.5 in. D 16 in. Weight, exclusive of packing materials: 28 pounds.
Electrical	Mains power: 115/230 Vac, 50-60 Hz, 50 VA max, 25 VA typical.
Environment	Operating temperature 10-50 deg. C. Relative Humidity 10-95%.
Telephone	RJ11 analog. FCC registration: EMC54S-15118-MD-E. Reqv: 0.8B. ULE10 1818.
Functional	User ID code length: 8 digits maximum, 1 digit minimum. Dialed number length: 28 digits maximum. Global Service Classes: 0 restricted 1&2 unrestricted. User Service Classes: 0 restricted, 1-9 unrestricted.
Reports	Authorized User ID list, selectable by range of user code. Call detail report, last in-first out, 5000 call sliding window. Active User Report, selectable by range of user code. Daily Active User Report.



FOR INFORMATION

CALL 1(800)885-8188

XIOX Corporation
577 Airport Blvd., Suite 700
Burlingame, CA 94010

Control No. 20019 1/93

MCI DETECTOR

Volume 1 Issue 1
Spring 1993

A publication
on the Issue of
Telecommunications
Fraud Protection

Welcome to the New *MCI* *Detector*

This is the first edition of the MCI Detect newsletter, DETECTOR.[SM] We have designed this publication to provide you with an overview of MCI's fraud prevention features, information on the latest fraudulent techniques, helpful hints on how to deal with fraud and feature stories on how we have helped customers.

A growing number of companies have been confronted with the toll fraud problem. While estimates vary, it is generally acknowledged that CPE-related fraud accounts for more than $1 billion each year in losses. The possibility of being hacked is very real.

MCI® has a long history of helping our customers deal with fraud problems including holding fraud prevention seminars, providing on-site consulting and supplying educational materials.

Now a new generation of anti-fraud measures have been developed to combat toll fraud. MCI Detect is a value-added service developed to "HELP YOU PUT THE FINGER ON FRAUD." It is a multi-faceted approach consisting of 4 key elements:

1. Customer Awareness & Education — Free to MCI Customers!

- Exclusive, award winning, fraud awareness video, "Invisible Criminals"
- MCI DETECTOR, quarterly informative newsletter
- Manual on easily compromised CPE features and functions (available mid-1993)
- "Hands on" consulting

2. Analysis of Customer Traffic—Free to MCI Customers!

- Analysis of customer's MCI domestically originated 800 traffic and outbound international to select high-fraud countries
- Customer notification of potentially fraudulent usage
- Assistance in resolving fraudulent situations

3. CPE Add-on Equipment through Affiliates Program

- 20% discount on MicroFrame and Xiox equipment for MCI customers
- Monitors any traffic routed through it: is not exclusive to the traffic of MCI or any other carrier
- Can be set to take corrective action without human intervention
- Has thresholds that can be tailored to individual business traffic patterns
- Monitors traffic on real time basis

4.Third-Party Insurance

- Coverage of all of customer's long distance traffic
- No MCI requirement for traffic volume commitment
- True insurance, not a service guarantee

For more information on how MCI Detect can help you put the finger on fraud speak with your MCI representative.

[illegible]

hints

MCI has a long history of helping our customers with fraud problems.

DISA

Fraud Method(s)—DISA is designed to allow remote access to a PBX and then originate an outbound call. As a result of this design, many PBX owners use DISA in lieu of Calling Cards; however, it is also used by call-sell operators in placing fraudulent calls.

The hackers are able to locate the DISA feature with the use of a "war dialer." The "war dialer" dials telephone numbers randomly, generally 800 numbers, until a modem or dial tone is obtained. After a number is found, hacking software is then used to search for valid authorization codes (auth codes). Codes are "frequently" but not always distributed to pirated voice mail systems and computer bulletin boards. The codes are usually distributed to a network of call-sell operators and may also be posted on bulletin boards and voice mail systems.

Fraud Solution (s)—There are many steps a PBX owner can take to prevent hackers from obtaining and fraudulently using the DISA feature. To begin with auth codes should be made as long as possible. At the very least a factor of 10.000 should exist between the active codes. For example, if there are 10 users the code should be at least 5 digits long (10 x 10.000 + 100.00 or 5 digits). Auth codes should be randomly scattered throughout the possible range but not easily defined (e.g. 1234 or 1111). Class of service restrictions should be applied to the auth codes. Only users with a truly legitimate need should be allowed International dialing through the DISA. A monitoring system should be set up to record DISA usage. Monitoring reports should show the number of times and minutes an auth code is used in a day. If possible, the dollar value of those calls should also be noted on the reports.

Voice Mail Boxes (VMB) As Bulletin Board

Fraud Method(s)—There are two types of VMB Systems fraud. The first type occurs when a hacker takes over a box and uses it to communicate with other hackers. This can be expensive if access is gained to the VMB System via an 800 number. In this situation, a hacker typically backs out the box password and changes it along with the greeting.

Fraud Solution(s)—To protect against a VMB being pirated the following steps should be taken:

- Do not allow administrative access via the phone. If telecom person can add, delete and change boxes via the phone, so can a hacker.
- Do not have active mail boxes that do not have an owner.
- Passwords should be at least 6 digits long.
- If possible, passwords should expire every 30-90 days.

Voice Mail Boxes (VMB) Garnering Dial Tone

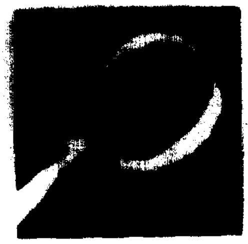
Fraud Method(s)—The second type of abuse involves garnering a PBX dial tone via the VMB. This is accomplished in two ways. Both methods can transfer out of the VMB to a phone on the system. If the PBX is not set up properly the transfer can be made directly to dial tone. In other instances the caller transfers to an extension. In some cases the extension may be on another PBX and require transmission over a tie line. If the tie line is not properly secured, dial tone can be retrieved and fraudulent calls placed. Finally, all PBXs have Trunk Access Codes (TACs) or Facility Access Codes (FACs). Technicians use these codes to make test calls. If allowed, a hacker can transfer out of the VMB to the TACs or FACs.

Fraud Solution (s)—Steps to Prevent PBX Fraud:

- Disabling the transferring out feature. This would restrict use to only receiving and retrieving messages.
- Limiting access to only 4-digit extensions, if transferring is allowed.
- Blocking 8 & 9 access (8 & 9 generally being draw dial tone numbers).
- Prohibiting trunk-to-trunk access from tie lines.
- Disallowing TAC and FAC access from the VMB.

MCI DETECT IN ACTION

Fraudulent Activity Discovered in Daily Analysis Report



MCI's Systems Integrity group recently came to the rescue of *The Times Record* in Brunswick, Maine. Karen Curia, an SI Staff Investigator, noticed in the daily analysis report that an unusually high number of calls to *The Times Record's* 800 number were coming in from the 212 area code. Karen realized that this pattern was out of the norm for *The Times Record,* and that the 212 area code further indicated that fraudulent activity was occurring. A hacker most likely had just cracked an access code into *The Times Record* PBX and sold the code to an individual who sold long distance service for a fee from payphones, a.k.a., a "call-sell" operation. She immediately called *The Times Record* and advised them to contact their equipment vendor to secure their system.

As a result, the fraud-related losses were kept to less than $500. Had this system of traffic analysis and prompt action by Karen not been in place, the loss could easily have been in the tens of thousands of dollars. Phyllis A. Thiboutot, Vice President and Treasurer of *The Times Record,* in commending Karen said, "I especially would like to forward my heartfelt thanks to Karen Curia for her work on our account; if it were not for her, we would have only discovered this problem today. MCI Investigations has done a superb job."

Congratulations Karen!

PRODUCT News Update

800 EXTENDED CALL COVERAGE℠

Beginning April 5, 1993, basic MCI 800 Service℠ and MCI Vision® 800 Service will include calls from Hawaii, U.S. Virgin Islands and Puerto Rico. Previously, these areas were part of Extended Call Coverage. Basic coverage will now include these areas automatically. This 800 service enhancement gives you the opportunity to explore new markets outside the United States.

Although the U.S. Virgin Islands and Puerto Rico do not currently account for large amounts of CPE or card fraud, there is a degree of certainty that inbound 800 from Puerto Rico will be used to access and defraud customers' equipment.

We advise our customers to block outbound calls to the 809 area code (809 contains the Caribbean countries) as well as to countries not included in the North American Numbering Plan, unless they have business reasons to allow the calls. This precaution will prevent, or at least limit, the most expensive fraudulent calls, the international ones. Blocking outbound, however, does not prevent the hacker from dialing in to your equipment via your 800 number.

MCI 800 service can be tailored so that 800 calls can originate from the areas you specify. This is called Tailored Call Coverage.℠ Using this capability, you can specify, by area code and exchange (also known as NPA & NXX), the areas you want to allow calls to originate from and the ones you do not. If, in the context of your business' requirements, you can prevent calls to your 800 number, from originating in a particular area, you have eliminated the possibility of fraud attacks via 800 access from that area.

As part of the changes to the areas included in Basic 800 coverage, MCI is waiving the Tailored Call Coverage (TCC) charge associated with blocking from April 1 until June 30. After June 30, there will be a $150 install charge to block calls from these areas, and a $110 change charge to include these areas (both one-time charges).

MCI is currently developing a list of NPA-NXX combinations from which significant amounts of fraud originate. This list will be made available to customers for consideration for possible exclusion from 800 coverage plans.

We hope that you have found the information contained in DETECTOR helpful in your efforts to prevent CPE-related fraud. Look for the next issue of DETECTOR in the third quarter of '93.

Control No. 24832 5/93

Reprinted from the ***CMA REVIEW***.

Are Thieves Using Your PBX?

Telephone fraud: an unfortunate tradition

by Jim Snyder

> ***For as long as fees have been levied for telephone service, thieves have schemed to avoid paying these charges particularly for long-distance calling. Unfortunately, this thievery is not only flourishing, but the individuals involved are constantly developing more sophisticated techniques for perpetrating fraud.***

Although telephone fraud existed prior to divestiture, it was less visible then because the associated costs were simply passed on to ratepayers. Following divestiture, however, the opportunities to make fraudulent long-distance calls multiplied.

> *The danger for the PBX owner is that the remote access authorization code will be compromised, enabling fraudulent calls to be originated through the PBX.*

Long-distance carriers entering the market relied on five and six digit personal identification numbers to provide customers with access to their networks. As these codes were relatively easy for hackers to break, the companies relying on them were extremely vulnerable. To combat this type of fraud, long-distance service providers improved their defenses. In response, the thieves changed the targets and methods of their thievery.

Remote access fraud

Perhaps the most critical issue facing telecommunications users today is remote access fraud, typically accomplished through Private Branch Exchanges (PBXs) and electronic Voice Mail Boxes (VMBs).

Any business that employs a PBX or a VMB in its telecommunications system can incur hundreds of thousands of dollars in losses (in a few days) at the hands of those intent on stealing services.

PBXs at the heart of the problem

The heart of the problem lies with the capabilities of PBXs and similar equipment: not only is the PBX able to transfer calls to extensions and provide access to the public switched network, it generally has a number of other useful features, such as remote access capability.

Remote access capability permits a user to dial an 800 number or a 7 or 10 digit number assigned to the Remote Access Unit (RAU) or the Direct Inward System Access (DISA) feature of a PBX, to remotely enter an authorization code through the telephone touch tone pad, and to obtain a dial tone. Then, if no egress restrictions are in place in the PBX, a call to any other telephone in the world is generated.

Compromised codes

The danger for the PBX owner is that the remote access authorization code will be compromised, enabling fraudulent calls to be originated through the PBX. Typically, the criminal who has gained possession of a remote access authorization code number will make a "free" inbound call to the PBX through the use of an 800 or a local number assigned to the customer's PBX, enter the compromised authorization code, and then dial the desired terminating number.

Once a PBX code has been compromised, it will be sold, then resold by each successive buyer again and again for as long as the code remains active. These codes are also used for "call-sell" operations in which long distance phone calls are "sold" to the public at pay phones and other locations.

> *The methods that are deployed against PBXs are limited only by the ingenuity of the criminals seeking to penetrate them.*

How hackers invade PBXs

The methods that are deployed against PBXs are limited only by the ingenuity of the criminals seeking to penetrate them. For example, if the lines are automatically answered by a call sequencer, which routes incoming calls, the PBX is at risk. A "hacker" can program his computer to generate calls to an 800 or a local number and learn the security codes resident in the PBX during the time that the call is on hold waiting to be answered. A computer isn't necessary, however, to identify a valid security code. Simple security codes are often discovered by hand.

Obscene calls signal fraud

Receiving numerous wrong or obscene phones calls could indicate another variety of PBX fraud. The caller may be taking advantage of a design flaw in

***PBX Fraud** (continued)*

older PBXs that returns a dial tone to the caller if the called party hangs up first. VMBs are also targets of this type of fraud since some systems provide a dial tone to the caller.

Owner is responsible

Because it is not possible to distinguish between a caller who is authorized to use the remote access facility of a PBX and the thief who happens to possess an authorization code, all telephone calls originating from the PBX are carried to the terminating number dialed, and the charges for the completion of the call are passed to the system owner.

The ability of some 800 service providers to supply the originating number of 800 calls may make those customers a less desirable target for remote access fraud because the perpetrator does not enjoy absolute anonymity. However, the sophisticated thief who is attempting to avoid detection may "loop," that is, sequentially dial through a number of different PBXs, and may combine the use of stolen credit cards and other illegal means to frustrate efforts to trace the actual origin of the call. The thief may also use public phone facilities that likewise cannot be traced back to him.

Take steps to "fraud-proof"

Because the mechanism that permits fraudulent calls to be made is equipment controlled by the customer, neither the long-distance service providers nor the local telcos will take responsibility for the losses resulting from remote access fraud. Consequently, telecommunications managers must take steps to ensure that their systems are secure. cma

Jim Snyder is an Executive Staff Member/Attorney in the Office of Corporate Systems Integrity for MCI Telecommunications.

Guard against PBX fraud

1. Understand all the capabilities of your PBXs and VMBs. The most logical source of information is the vendor who sold or services the equipment. A vendor should be able to describe the fraud-defensive capabilities of a given system.
2. Delete all authorization codes that may have been programmed into the PBX or VMB for testing and service.
3. Frequently audit and change all active codes in a PBX or a VMB. Those no longer authorized – particularly codes which were assigned to former employees, summer interns, and others who are no longer valid users – should be deactivated immediately. Access to authorization codes should always be limited to those who truly have a "need to know."
4. Treat authorization codes just as you would credit card numbers. Each code should be assigned individually, and employees should be instructed as to their confidentiality. For example, they must be told that codes should never be written down on anything which might be discarded, lost or seen by an unauthorized person. Caution them about using pay telephones at airports, hotels, or bus stations: someone may attempt to observe the dialing sequence of the authorization code.
5. Consider replacing the remote access function in the PBX with a virtual private network card which minimizes the company's exposure to fraud. If the remote access function in the PBX is retained, the authorization numbers selected as DISA or RAU codes should be the longest numerical sequence the PBX is designed to handle and choose entirely at random. Because telephone extension numbers, Social Security numbers, and employee identification numbers are easily discovered by thieves, avoid using them as authorization codes.
6. Inform all employees that the person on the other end of a phone conversation may not be the person he or she claims to be. Perhaps a thief, who is trying to learn more about the employee's phone system in order to defraud the company, is posing as a legitimate contact. Remind them that "dumpster divers" regularly scour trash receptacles to obtain discarded company information that may include remote call authorization codes and other proprietary material.
7. Tailor access the PBX to conform strictly with the needs of the company. International and those portions of domestic long distance access that the company does not use should be blocked. If feasible, remote access calling capability should be completely shut down during off-hours and weekends.
8. Establish an unpublished number for the remote access unit/direct inward system access, and program the PBX to wait at least 5 rings before responding to the call.
9. Review billing information to identify unauthorized calling patterns. 800 call detail, a billing option provided by certain 800 service providers, helps identify fraudulent calls to the PBX and/or VMB. Numerous inbound calls of very short duration usually indicate hacking activity, while outbound calls of long duration often, although not always, reflect fraudulent usage. High volumes of calls during off-peak hours (late night and early morning) are also symptoms of possible fraud.
10. Finally, avoid using a steady tone as the prompt to input an authorization code. Instead, use a voice recording or no prompt at all. Whenever an invalid authorization code is entered, the call should either be terminated or routed to a switchboard operator.

MCI Systems Integrity Customer Support Program

MCI